REMARKS

This application has been carefully reviewed in light of the Office Action dated May 23, 2007. Claims 1 to 15 remain in the application, of which Claims 1, 2, 11 and 13 to 15 are independent. Reconsideration and further examination are respectfully requested.

Applicant wishes to thank the Examiner for the courtesies and thoughtful treatment accorded Applicant's undersigned representative during the August 20, 2007 telephonic interview. This amendment has been prepared in accordance with the discussions of that interview.

In the Office Action, the specification was objected to as allegedly introducing new matter regarding the term "continually". Claims 1 to 15 were rejected under 35 U.S.C. § 112, first paragraph and second paragraph, also with regard to the term "continually". Without conceding the correctness of the objections or rejections, the term "continually" has been amended in the claims to correspond more closely with the specification. Reconsideration and withdrawal of the objections and rejections are respectfully requested.

Claims 1 to 15 were rejected under 35 U.S.C. § 102(e) over U.S. Patent No. 6,526,506 (Lewis). Reconsideration and withdrawal of the rejections are respectfully requested.

The present invention relates to configuring a new wireless network between a client terminal and an access point device. In the invention, the client terminal sends a network configuration request to the access point for configuring the new wireless network. A first wireless communication link that does not require and authentication

process is established between the client terminal and the access point device. That is, a low level encryption method that utilizes, for example, a password or PIN is used to establish the first encrypted communication link. The access point device then determines whether or not the client terminal is authorized to be configured into a new network, and if so, sends authentication data to the client terminal utilizing the first wireless (low level) encryption communication link. The first wireless communication link is then discarded in response to the sending of the authentication data. Then, a second wireless communication link that requires an authentication process is established using the authentication data sent to the client terminal, after the first wireless communication link is discarded.

Referring specifically to the claims, Claim 1 is directed to a network configuration method of configuring a wireless network, comprising an access point device receiving a network configuration request for configuring a new wireless network comprising the access point device and at least one client terminal, a first link establishing step of establishing, between the access point device and a client terminal, a first wireless communication link through a first encrypted communication that does not require an authentication process, a determination step of determining whether or not the client terminal is authorized to be configured in the network with the access point device, a sending step of, if the determination step determines that the client terminal is authorized to be configured in the network with the access point device, the access point device sending authentication data from said access point device to said client terminal in a state where the first wireless communication link through said first encrypted communication is established, a link discarding step of discarding the first wireless communication link through said first encrypted communication between said access point device and said

client terminal in response to the sending of the authentication data to the client terminal by the access point device at said sending step, and a second link establishing step of establishing, between said access point device and said client terminal, a second wireless communication link through a second encrypted communication that requires an authentication process using the authentication data sent to said client terminal after discarding the first communication link at said link discarding step.

Claim 2 is a method claim directed to the access point device, while Claim 14 is an apparatus claim directed to the access point device, each of which include features substantially corresponding to Claim 1. Claim 11 is a method claim directed to the client terminal side of the invention, while Claim 15 is an apparatus claim that substantially corresponds to Claim 11.

The applied art of Lewis is not seen to disclose or to suggest the features of Claims 1, 2, 11 and 13 to 15, and in particular, is not seen to disclose or to suggest at least the features of an access point device determining whether or not a client terminal requesting that a new wireless communication be configured between the client terminal and the access point device is authorized to be configured in the network, and if so, sending authentication data to the client terminal, whereby a first wireless communication link that does not require an authentication process is discarded and a second wireless communication link is established between the client terminal and the access point device through a second encrypted communication that requires an authentication process using the authentication data received from the access point device after discarding the first wireless communication link.

Lewis is to disclose two embodiments. In one embodiment, a device sends a message to an access point using a MASTER key. The access point recognizes that the MASTER key and simply forwards the message on to a network backbone to a key distribution server. The key distribution server then issues an ENCRYPT key to the device. The device can then use the ENCRYPT key to send messages to the access point device. Thus, in this embodiment, the first wireless communication link is not established. Moreover, the authentication data (ENCRYPT key) is sent by the key distribution server to the device and not by the access point. Additionally, the ENCRYPT key is not sent by the access point in a state where the first wireless communication link is established. Presumably, since the access point merely forwards the message to the key distribution server, any "link" that may have been established between the device and the access point when the message containing the MASTER key was transmitted is terminated when the message is forwarded onto the backbone.

In another embodiment, the device may attempt to communication with the access point using an ENCRYPT key that may have been changed. In this embodiment, the device sends a message with ENCRYPT key to the access point. The access point recognizes the ENCRYPT key as being outdated. Therefore, the access point issues the latest ENCRYPT key to the device by encrypting the latest key using the outdated key. The device then uses the latest key to resend the message to the access point using the latest (updated) ENCRYPT key. Thus, while this embodiment may establish two separate communication links, as Applicant understands Lewis, both links are an encryption process that require authentication. That is, the first message is encrypted with an encryption key that presumably requires authentication. The second message is encrypted with the new

encryption key and it likewise presumably requires authentication. This is a problem where the device simply does not have the ENCRYPT key to begin with, or the MASTER key. The invention aims to address this problem.

In the invention, a network configuration technique is provided for devices that do not have the required credentials. The invention establishes a first communication link using a first (low level) encrypted communication that does not require an authentication process. As briefly discussed above, the device merely uses a PIN or password for the low level encrypted communication. The access point device can then look-up to see if the device was previously registered as being allowed to be configured in a wireless network with the access point. This can be done by merely referring to a table that includes the password, and perhaps a device ID. If the access point determines that the client terminal is authorized to be configured in the network, then the low level encrypted communication is used to provide authentication data to the device, which can then be used to establish a second wireless communication link with a high level of encryption. Thus, the invention makes it easier for devices without having prior credentials to be configured into a secure wireless network, and does so without the need for separate key distribution servers. Accordingly, the invention is not believed to be anticipated by Lewis.

Bluetooth merely teaches the use of encryption keys and an authentication key in wireless communications. However, the Bluetooth standard is not seen to teach the foregoing features of the claimed invention.

In view of the forgoing amendments and remarks, all of Claims 1 to 15 are believed to be allowable.

No other matters having been raised, the entire application is believed to be in condition for allowance and such action is respectfully requested at the Examiner's earliest convenience.

Applicant's undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

/Edward Kmett/

Edward A. Kmett
Attorney for Applicant
Registration No. 42,746

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200

FCHS_WS 1536453v1